CONTENTS

- Footprinting Concepts
- Footprinting through search engines
- Footprinting through Web services
- Footprinting through social networking sites
- Footprinting tools
- Footprinting countermeasures

Footprinting Concepts

- An essential aspect of footprinting is identifying the level of risk associated with the organization’s publicly accessible information. Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting, you can find a number of opportunities to penetrate and assess the target organization’s network.
- Types of Footprinting
  - Passive Footprinting

    Passive footprinting involves gathering information about the target without direct interaction. It is mainly useful when the information gathering activities are not to be detected by the target. Performing passive footprinting is technically difficult, as active traffic is not sent to the target organization from a host or anonymous hosts or services
  - Active Footprinting

Active footprinting involves gathering information about the target with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network. Active footprinting requires more preparation than passive footprinting, as it may leave traces that may alert the target organization.

Information Obtained in Footprinting

Organization Information:

- Employee details (employee names, contact addresses, designations, and work experience)
- Addresses and mobile/telephone numbers
- Branch and location details
- Partners of the organization
- Web links to other company-related sites
- Background of the organization
- Web technologies
- News articles, press releases, and related documents
- Legal documents related to the organization

Information Obtained in Footprinting

Network Information:

- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records and related information

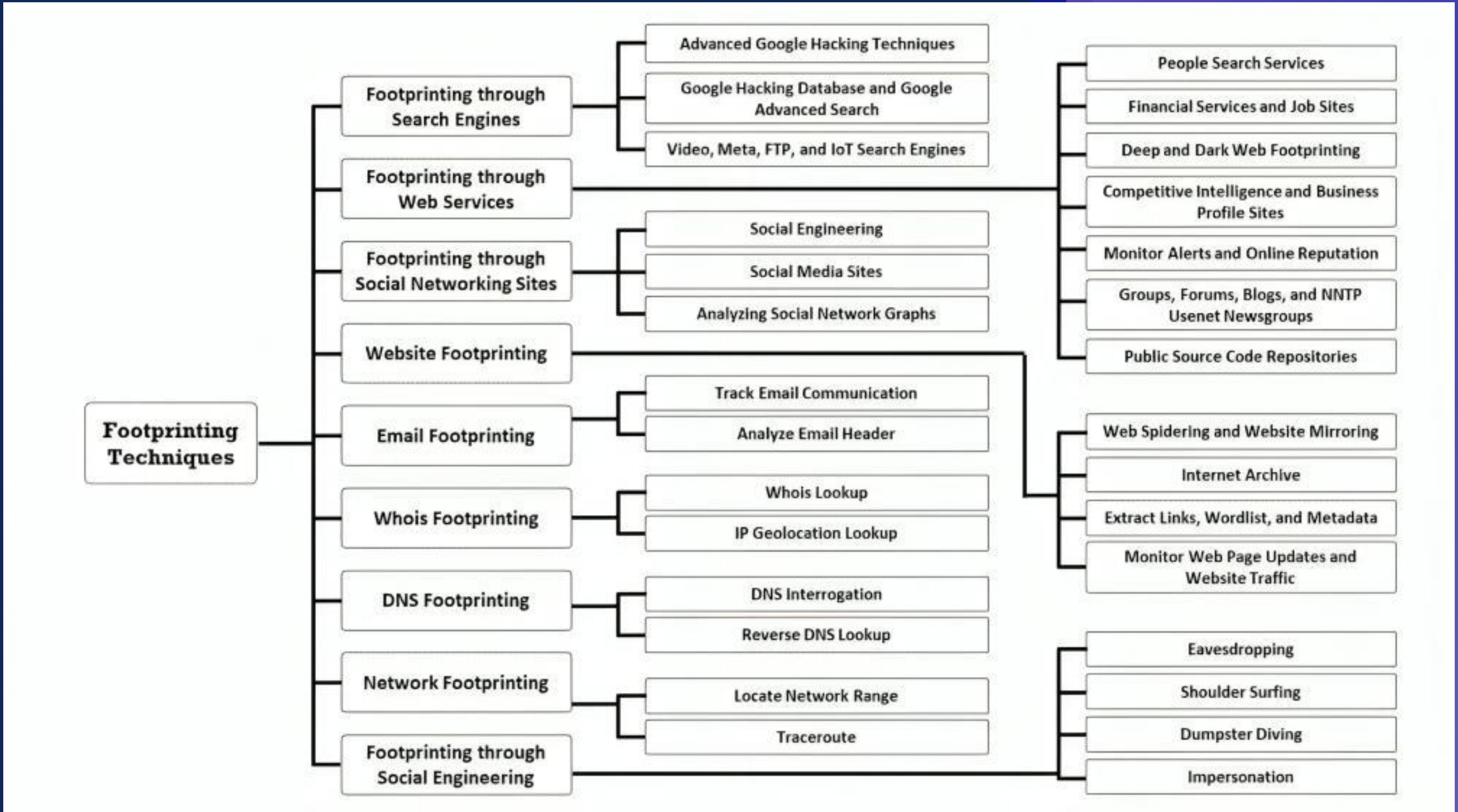
System Information:

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames, passwords, and so on.

Footprinting Threats

- **Social Engineering**: Without using any intrusion methods, hackers directly and indirectly collect information through persuasion and other means. Hackers gather crucial information from willing employees who are unaware of the hackers' intent.
- **System and Network Attacks**: Footprinting enables an attacker to perform system and network attacks. Thus, attackers can gather information related to the target organization's system configuration, the operating system running on the machine, and so on.
- **Information Leakage**: Information leakage poses a threat to any organization. If sensitive information of an entity falls into the hands of attackers, they can mount an attack based on the information or alternatively use it for monetary benefit.
- **Privacy Loss**: Through footprinting, hackers can access the systems and networks of the organization and even escalate the privileges up to admin levels, resulting in the loss of privacy for the organization as a whole and for its individual personnel.
- **Corporate Espionage**: Corporate espionage is a central threat to organizations, as competitors often aim to attempt to acquire sensitive data through footprinting. Through this approach, competitors can launch similar products in the market, alter prices, and generally undermine the market position of a target organization.
- **Business Loss**: Footprinting can have a major effect on organizations such as online businesses and other e-commerce websites as well as banking and finance-related businesses.

Footprinting Methodology



- Footprinting Techniques
  - Footprinting through Search Engines
    - Advanced Google Hacking Techniques
    - Google Hacking Database and Google Advanced Search
    - Video, Meta, FTP, and IoT Search Engines
  - Footprinting through Web Services
    - People Search Services
    - Financial Services and Job Sites
    - Deep and Dark Web Footprinting
    - Competitive Intelligence and Business Profile Sites
    - Monitor Alerts and Online Reputation
    - Groups, Forums, Blogs, and NNTP Usenet Newsgroups
    - Public Source Code Repositories
  - Footprinting through Social Networking Sites
    - Social Engineering
    - Social Media Sites
    - Analyzing Social Network Graphs
  - Website Footprinting
    - Web Spidering and Website Mirroring
    - Internet Archive
    - Extract Links, Wordlist, and Metadata
    - Monitor Web Page Updates and Website Traffic
  - Email Footprinting
    - Track Email Communication
    - Analyze Email Header
  - Whois Footprinting
    - Whois Lookup
    - IP Geolocation Lookup
  - DNS Footprinting
    - DNS Interrogation
    - Reverse DNS Lookup
  - Network Footprinting
    - Locate Network Range
    - Traceroute
  - Footprinting through Social Engineering
    - Eavesdropping
    - Shoulder Surfing
    - Dumpster Diving
    - Impersonation

Footprinting Through Search Engine

- Search engines are the main sources of key information about a target organization. They play a major role in extracting critical details about a target from the Internet. Search engines use automated software, i.e., crawlers, to continuously scan active websites and add the retrieved results in the search engine index that is further stored in a massive database. When a user queries the search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed according to their relevance. Many search engines can extract target organization information such as technology platforms, employee details, login pages, intranet portals, contact information, and so on. The information helps the attacker in performing social engineering and other types of advanced system attacks.

- A Google search could reveal submissions to forums by security personnel, disclosing the brands of firewalls or antivirus software used by the target. This information helps the attacker in identifying vulnerabilities in such security controls.

- Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

Google Dorking

Filter	**Description**	**Example**
allintext	Searches for occurrences of all the keywords given.	allintext:"keyword"
inurl	Searches for a URL matching one of the keywords.	inurl:"keyword"
intitle	Searches for occurrences of keywords in title all or one.	intitle:"keyword"
site	Specifically searches that particular site and lists all the results for that site.	site:"www.google.com"
filetype	Searches for a particular filetype mentioned in the query.	filetype:"pdf"
link	Searches for external links to pages.	link:"keyword"
cache	Shows the version of the web page that Google has in its cache.	cache: www.google.com

Shodan

ip:	Filter results by specific IP address.
asn:	Filter results by specific ASN ID.
hostname:	Filter results by specific hostname.
port:	Filter results by specific port number of service.
net:	Filter results from specified CIDR block.
isp:	Filter results by devices assigned a particular address (space) from a specified ISP.
city:	Filter results by specific city.
country:	Filter results by specific two-digit country code.
os:	Filter results by particular OS.
product:	Filter results by particular software.
version:	Filter results by specified version of software.

Footprinting Through Web Services

- **Netcraft**

Source: https://www.netcraft.com

Netcraft provides Internet security services, including anti-fraud and anti-phishing services, application testing, and PCI scanning. They also analyze the market share of web servers, operating systems, hosting providers and SSL certificate authorities, and other parameters of the Internet.

- **Pentest-Tools Find Subdomains**

Source: https://pentest-tools.com

Pentest-Tools Find Subdomains is an online tool used for discovering subdomains and their IP addresses, including network information and their HTTP servers.

Footprinting through Social Networking Sites

People Search Service - Spokeo

Source: https://www.spokeo.com

Attackers can use the Spokeo people search online service to search for people belonging to the target organization. Using this service, attackers obtain information such as phone numbers, email addresses, address history, age, date of birth, family members, social profiles, and court records.

theHarvester

theHarvester is a tool designed to be used in the early stages of a penetration test. It is used for open-source intelligence gathering and helps to determine a company's external threat landscape on the Internet. The following command to enumerate users on LinkedIn:

```
theHarvester –d microsoft –1 200 –b linkedin
```

the following command to extract email addresses of microsoft.com using the Baidu search engine:

```
theharvester –d microsoft.com –1 200 –b baidu
```

Whois Lookup

- Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRS) maintain Whois databases, which contain the personal information of domain owners.
- Whois services such as http://whois.domaintools.com and https://www.tamos.com can help perform Whois lookups.

- SecurityTrails

Source: https://securitytrails.com

SecurityTrails is an advanced DNS enumeration tool capable of creating a DNS map of the target domain network. It can enumerate both current and historical DNS records such as A, AAAA, NS, MX, SOA, and TXT, which helps in building the DNS structure. It also enumerates all the existing subdomains of the target domain using brute-force techniques.

Footprinting Tools

- ***Maltego***

Source: https://www.maltego.com

Maltego is an automated tool that can be used to determine the relationships and real world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.

- ***Recon-ng***

Recon-ng is a web reconnaissance framework with independent modules for database interaction that provides an environment in which open-source web-based reconnaissance can be conducted.

- ***Censys***

https://censys.com/

Footprinting Countermeasures

- Restrict the employees' access to social networking sites from the organization's network.
- Configure web servers to avoid information leakage.
- Educate employees to use pseudonyms on blogs, groups, and forums.
- Do not reveal critical information in press releases, annual reports, product catalogs, etc.
- Limit the amount of information published on a website or the Internet.
- Use footprinting techniques to discover and remove any sensitive information that is publicly available.
- Prevent search engines from caching a web page and use anonymous registration services.
- Develop and enforce security policies such as information security and password policies to regulate the information that employees can reveal to third parties.
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers.
- Disable directory listings in the web servers.
- Encrypt and password-protect sensitive information.
- Do not enable protocols that are not required.
- Always use TCP/IP and IPsec filters for defense in depth.